

**STATE OF SOUTH CAROLINA**

**INDEPENDENT AUDITORS' REPORT ON  
COMPLIANCE AND ON INTERNAL CONTROL OVER  
FINANCIAL REPORTING BASED ON AN AUDIT OF  
GENERAL PURPOSE FINANCIAL STATEMENTS  
PERFORMED IN ACCORDANCE WITH  
*GOVERNMENT AUDITING STANDARDS***

**JUNE 30, 2001**

## **CONTENTS**

### **PAGE**

INDEPENDENT AUDITORS' REPORT ON COMPLIANCE AND ON INTERNAL CONTROL OVER FINANCIAL REPORTING BASED ON AN AUDIT OF GENERAL PURPOSE FINANCIAL STATEMENTS PERFORMED IN ACCORDANCE WITH <i>GOVERNMENT AUDITING STANDARDS</i>	1
<b>REPORTABLE CONDITIONS</b>	
01-1 Financial Reporting Employment Security Commission	3
01-2 Accounts Payable Employment Security Commission	3
<b>OTHER MATTERS</b>	
01-3 Internet Tax Filing Reconciliation Department of Revenue	4
01-4 Physical Access Controls Department of Revenue	4
01-5 Information Security State Treasurer's Office	4
01-6 Disaster Recovery/Business Continuity Planning Office of Information Resources	5
01-7 Security Policies and Procedures Department of Health and Environmental Control	5
01-8 Granting/Removal of Employee Access – AIMS Department of Health and Environmental Control	6
<b>SUMMARY OF PRIOR FINDINGS</b>	7
<b>MANAGEMENTS' RESPONSES</b>	8



INDEPENDENT AUDITORS' REPORT ON COMPLIANCE AND ON INTERNAL  
CONTROL OVER FINANCIAL REPORTING BASED ON AN AUDIT OF  
GENERAL PURPOSE FINANCIAL STATEMENTS PERFORMED IN  
ACCORDANCE WITH GOVERNMENT AUDITING STANDARDS

The Honorable Jim Hodges, Governor  
and  
Members of the General Assembly  
State of South Carolina  
Columbia, South Carolina

We have jointly audited the general purpose financial statements of the State of South Carolina as of and for the year ended June 30, 2001, and have issued our report thereon dated November 30, 2001. We did not jointly audit the financial statements of certain blended component units and agencies of the primary government, which statements reflect the indicated percent of total assets and other debits and total revenues, respectively, of the Special Revenue (55% and 18%), Enterprise (99% and 95%), Internal Service (70% and 88%), Pension Trust (100% and 100%), Investment Trust (100% and 100%), Higher Education (100% and 100%), and Agency (19% of assets and other debits) Funds, General Fixed Assets Account Group (11% of assets and other debits), and the General Long-Term Obligations Account Group (61% of assets and other debits). We also did not jointly audit the financial statements of the discretely presented component units. Those financial statements were audited by other auditors, including the Office of the State Auditor and Deloitte & Touche LLP acting separately, whose reports have been furnished to us, and our opinion, insofar as it relates to the amounts included for those component units and agencies, is based solely upon the reports of other auditors. Deloitte & Touche LLP acting separately has audited 100% of the total assets and other debits and total revenues of the Investment Trust Fund, 3% and less than 1% of the total assets and other debits and total revenues, respectively, of the Special Revenue Funds, and 23% of the assets and other debits of the General Long-Term Obligations Account Group. The Office of the State Auditor acting separately has audited 38% and 44% of the total assets and other debits and total revenues of the Higher Education Funds.

We conducted our joint audit in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. The financial statements of the discretely presented component units identified in Note 1(a) to the general purpose financial statements of the State of South Carolina were not audited in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States.

The Honorable Jim Hodges, Governor  
and  
Members of the General Assembly  
State of South Carolina

### Compliance

As part of obtaining reasonable assurance about whether the State of South Carolina's general purpose financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grants, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit and, accordingly, we do not express such an opinion. The results of our tests disclosed instances of noncompliance that are required to be reported under *Government Auditing Standards* and which are described in findings 01-1 and 01-2.

### Internal Control Over Financial Reporting

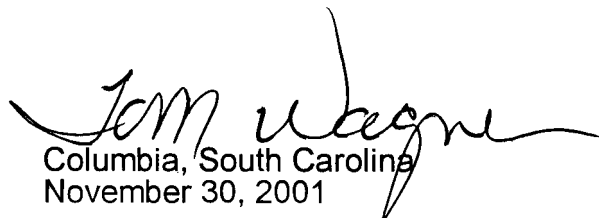
In planning and performing our audit, we considered the State of South Carolina's internal control over financial reporting in order to determine our auditing procedures for the purpose of expressing our opinion on the general purpose financial statements and not to provide assurance on the internal control over financial reporting. Our consideration of the internal control over financial reporting would not necessarily disclose all matters in the internal control that might be material weaknesses. A material weakness is a condition in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that misstatements in amounts that would be material in relation to the financial statements being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions. We noted no matters involving internal control over financial reporting and its operation that we consider to be material weaknesses.

However, we noted other matters involving the internal control over financial reporting that are described in findings 01-3 – 01-8.

This report is intended solely for the information and use of the Governor, Members of the General Assembly, the governing body and management of State agencies and the cognizant federal audit agency, and is not intended to be and should not be used by anyone other than these specified parties.

**Deloitte + Touche, LLP**

Columbia, South Carolina  
November 30, 2001

  
Columbia, South Carolina  
November 30, 2001

**REPORTABLE CONDITIONS**

## **01-1 Financial Reporting**

### **Employment Security Commission**

The Comptroller General's Policies and Procedures Manual (STARS Manual) section 2.1.7.20 states that agencies with federal subfunds are required to perform monthly reconciliations between the State's Comptroller General (CG) CSA 467CM report (Trial Balance by Subfund, Project and GLA) and the agency's records for each project and phase code. Through our discussion with Employment Security Commission (ESC) personnel, we determined that ESC did not perform monthly reconciliations for fiscal year 2001 as required. As a result, there is no process in place to detect and identify variances between ESC's books and the CG's accounting records. We noted no differences when we performed a reconciliation between the ESC's books and the CG's accounting records during the course of our audit. A similar comment was included in our prior report.

We again recommend that ESC prepare monthly reconciliations of agency accounting records to the CG reports in a timely manner. The reconciliations should be documented in writing, in an easily understandable format with all supporting working papers maintained for audit purposes including the signatures of the preparer and reviewer and the dates of preparation and review. The reconciliation of parallel accounting systems assures that transactions are accurately processed by both the agency and the CG, strengthens the internal accounting controls for both the agency and the State, and assures proper classification of transactions presented in the State's financial statements.

See agency response at page 8.

## **01-2 Accounts Payable**

### **Employment Security Commission**

We noted that the Employment Security Commission (ESC) failed to review vouchers paid in fiscal month 02 of the fiscal year 2002 when preparing the accounts payable closing package. The GAAP Closing Procedures Manual (GAAP Manual) states that agencies must review vouchers paid in fiscal months 01 and 02 of the new fiscal year and invoices the agency plans to pay in the new fiscal year for goods/services received prior to June 30. We reviewed fiscal month 02 vouchers and determined that no vouchers had met the requirement to be included in the closing package. We determined that ESC excluded fiscal month 02 because the agency was relying on a schedule from the State Comptroller General's Office (CG) which included vouchers for fiscal month 01 only.

We recommend that ESC develop and implement procedures for reviewing subsequent year vouchers to ensure that the vouchers are accounted for in accordance with GAAP Manual instructions for preparing the accounts payable closing package. The agency should use internally generated data when preparing the closing package and may use external data (e.g. the schedule provided by the CG) only after determining the accuracy and completeness of that data.

See agency response at page 8.

**OTHER MATTERS**

### **01-3 Internet Tax Filing Reconciliation**

#### **Department of Revenue**

The Department of Revenue (DOR) performs a reconciliation to ensure that all credit card payments for taxpayers who file returns on the internet are processed on the mainframe. A daily reconciliation of all monies received via credit card transactions is also performed. However, we found that DOR does not reconcile all internet returns filed (including refund and zero tax due filings) to the mainframe. The lack of a control activity to ensure all internet returns received are processed appropriately on the mainframe results in an increased risk that financial data from those returns may be processed inaccurately.

We recommend that appropriate internal control procedures be established for the processing of internet filings. The control activity should ensure that transactions are reconciled to the mainframe in such a manner as to ensure completeness, accuracy and validity of all processing of Internet-filed returns. Once a control activity has been identified and put into action, specific personnel need to be assigned responsibility for the monitoring of the control activity to ensure the control is operating appropriately.

See agency response at page 10.

### **01-4 Physical Access Controls**

#### **Department of Revenue**

DOR plans to locate an exercise area directly next to its network equipment room. All Local Area Network equipment is located inside the Network Equipment Room and is separated from the Exercise Room by partitions and heavy-duty mesh wire walls. The wire walls for the Network Equipment Room have a secured door that is locked with only key access. Keys are only provided to authorized personnel. While key locks can provide adequate physical security, risks related to unauthorized access increase since keys can be copied. Unsupervised off-hour access to the area that contains the network servers and the SQL servers creates a risk of damage to these servers.

We recommend that DOR include a combination locking mechanism for all entrances where computer processing hardware is located. Passwords and keys should be given only to authorized information system employees. Passwords should be changed on a 30-day cycle and immediately after employees with access to such areas are terminated.

See agency response at page 11.

### **01-5 Information Security**

#### **State Treasurer's Office**

We determined that programmers at the State Treasurer's Office (STO) have access to JCL, object, source code and key datasets (specifically, the warrant file, contingent checks, and Department of Social Services checks). Programmers also have RACF group special authorization that is excessive. We have identified the following mitigating controls:

- The programming support group for the STO is very small, thereby allowing programmer accountability to be maintained.
- Although programmers have access to JCL, they do not have access to the signature libraries. Therefore, they cannot print checks; the job would abend (have an abnormal ending).



### **State Treasurer's Office (Continued)**

- The warrant file (which is a listing of checks and amounts to be paid) is compared to the daily cash register. If amounts do not agree it is a signal that data could have been manipulated or lost.

While these mitigating controls minimize the risk inherent in granting unrestricted access to programmers, the controls are largely detective and inefficient.

We recommend that the STO take steps to restrict the ability of programming personnel to directly alter production program and data files. Change management procedures should be developed that require the migration of program modifications to be approved by management, and performed by individuals who are independent of the programming area. At a minimum, all changes to production programs by information system (IS) personnel should be documented and reviewed by IS management for reasonableness on a regular basis.

We also recommend that excessive access granted to programmers through RACF group special authorization be removed. Security administration personnel should coordinate a periodic review of all user access capabilities within RACF.

See agency response at page 12.

## **01-6 Disaster Recovery/Business Continuity Planning**

### **Office of Information Resources**

In our fiscal year 2000 report we disclosed several weaknesses in the disaster recovery plan for the State Budget and Control Board Office of Information Resources (OIR). OIR has since contracted with a private entity for disaster recovery services. However this disaster recovery plan was not tested during fiscal year 2001. Scheduled testing of coordinated business critical department recovery plans should be performed to assure the ability to continue normal operations after an information systems interruption. We reviewed a draft copy of OIR's disaster recovery plan and determined that it was incomplete. OIR personnel told us that the plan could not be completed until the needed information is received from all State agencies that run jobs on OIR processors.

We recommend that OIR test the disaster recovery plan to ensure usability. Results of testing will aid in the review and update of the plan. We also recommend that OIR complete the plan and address both technological and manual business processes required for successful continuity of critical operations. Finally, OIR should incorporate all agencies and associated computing platforms in its plan.

See agency response at page 13.

## **01-7 Security Policies and Procedures**

### **Department of Health and Environmental Control**

The South Carolina Department of Health and Environmental Control (DHEC) does not have formally documented security policies that are updated and communicated to all personnel. An effective written information security policy is important to ensure that information system resources are effectively secured according to the degree of related risk. Accompanying procedures are also necessary to ensure security controls are implemented according to management's objectives, and are applied consistently and effectively.

**Department of Health and Environmental Control (Continued)**

We recommend that DHEC develop formal information security policies and accompanying procedures and communicate the policies to all employees with access to computer systems. In developing the policies, management should:

- Review the types and uses of all system resources and classify them according to importance and sensitivity, and
- Provide user education and communication of the security policies.

DHEC should, at a minimum, document and implement security administration procedures which:

- Assign responsibility for maintaining and enforcing security administrative procedures.
- Define user responsibility for the information used and processed.
- Require written management approval for granting access authorities and ensure timely changes to employee access after terminations or transfers.
- Specify password requirements.
- Provide for periodic review of security violations.

See agency response at page 14.

**01-8 Granting/Removal of Employee Access – AIMS****Department of Health and Environmental Control**

During our review of procedures used for administering employee access to system resources, we noted that security administration procedures do not ensure that access capabilities are changed as employees leave a department and move into another department within DHEC. Accordingly, unauthorized or unintentional access to computer resources could occur. Currently, there is minimal monitoring when employees change departments, and there are no formal procedures for removing unnecessary responsibilities.

We recommend that DHEC implement procedures to ensure that systems access for transferred or terminated employees is updated or removed in a timely manner. Consider generating a list of terminated and transferred employees from the Human Resource system on a monthly basis and distributing the list to the data base administration manager for access updating/removal.

See agency response at page 15.

## **SUMMARY OF PRIOR FINDINGS**

During the current engagement, we reviewed the status of corrective action taken on each of the findings in the prior report on compliance and on internal control over financial reporting at the general purpose financial statement level, dated December 1, 2000 to determine if the conditions still existed. Based on our audit procedures we determined that adequate corrective action had been taken on each of the findings except as follows:

<u>Prior Finding</u>	<u>Repeated in</u>
Accounts Payable Employment Security Commission	01-2
Financial Reporting Employment Security Commission	01-1
Internet Tax Filing Reconciliation Department of Revenue	01-3
Disaster Recovery/Business Continuity Planning Office of Information Resources	01-6
Security Policies and Procedures Department of Health and Environmental Control	01-7
Granting/Removal of Employee Access – AIMS Department of Health and Environmental Control	01-8

## **MANAGEMENTS' RESPONSES**



www.sces.org

COMMISSIONERS  
J. William McLeod  
McKinley Washington, Jr.  
Carole C. Wells

EXECUTIVE DIRECTOR  
C. Michael Mungo  
(803) 737-2617  
mmungo@scs.org

1550 Gadsden Street  
Post Office Box 995  
Columbia, South Carolina 29202

January 25, 2002

Mr. Richard H. Gilbert, Jr.  
Director of State Audits  
State Auditor's Office  
1401 Main Street, Suite 1200  
Columbia, South Carolina 29211

Dear Mr. Gilbert:

As requested, the following is the response regarding the State of South Carolina's statewide joint audit of the general purpose financial statements, relating to the Fiscal Year 2000-2001 financial packages submitted by the Commission:

Financial Reporting: We concur with the recommendation for monthly reconciliation of agency accounting records with the State's Comptroller General CSA467 CM Report.

The agency has continued to expand its monthly reconciliation process and is working to reconcile its accounting records with the State Comptroller General's CSA 467 CM Report (Trial Balance by Sub-fund, Project and GLA). We are currently creating and expanding our electronic spreadsheets of agency accounting records and Comptroller General's reports to an understandable format. We are continuing to upgrade the current electronic spreadsheets to an automated process by the end of Fiscal Year 2001-2002.

Accounts Payable: We concur with the recommendation to develop a systemic approach to ensure all fiscal month 01 and 02 vouchers are reviewed for all agency funds.

In Fiscal Year 2000-2001, we developed a daily report listing all vouchers paid over \$250 for our administrative funding. We will expand this report to include our Unemployment Insurance sub-funds for 2001-2002. This new report will ensure accuracy when collecting information for the Accounts Payable Closing Package for all fund sources. We are coordinating with our programmer at this time to expand our current report to include all fund sources.

If there are any questions, or if additional information is needed, please contact the Finance Department, at (803) 737-2560.

Sincerely,

Billy R. Martin  
Manager of Fiscal Systems

Your  
**onestop**  
to a New Career!

BRM:sc

-8-

---

State of South Carolina  
Department of Revenue  
301 Gervais Street, P.O. Box 125, Columbia, South Carolina 29214

---

Mary McKissock  
Senior Accountant  
Deloitte & Touche  
Columbia, South Carolina

RE: Second Submittal of May 2001 Audit Responses

January 25, 2002

Ms. McKissock,

Attached are the audit responses to your May 2001 audit. I have modified my responses to reflect the second draft of comments I received from D&T.

Sincerely,



Michael D. Garon  
CIO, Department of Revenue

Copy to:  
State Auditor's Office  
1401 Main Street, Suite 1200  
Columbia, SC 20201

---

State of South Carolina  
Department of Revenue  
301 Gervais Street, P.O. Box 125, Columbia, South Carolina, 29214

---

### **01-3 Internet Tax Filing Reconciliation**

#### **Department of Revenue**

The Department of Revenue (DOR) performs a reconciliation to ensure that all credit card payments for taxpayers who file returns on the Internet are processed on the mainframe. A daily reconciliation of all monies received via credit card transactions is also performed. However, we found that DOR does not reconcile all Internet returns (including refund and zero tax due filings) to the mainframe. The lack of a control activity to ensure all internet returns received are processed appropriately on the mainframe results in an increased risk that financial data from those returns may be processed inaccurately.

We recommend that appropriate internal control procedures be established for the processing of Internet filings. The control activity should ensure that transactions are reconciled to the mainframe in such a manner as to ensure completeness, accuracy and validity of all processing of internet-filed returns. Once a control activity has been identified and put into action, specific personnel need to be assigned responsibility for the monitoring of the control activity to ensure the control is operating appropriately.

#### **Management Comments**

##### **DOR: Michael Garon - CIO**

The Department of Revenue's Internet SCNET program was designed to emulate the IRS Internet program. At the beginning of the year the process starts out with control number 1 for a batch. Each additional batch is incremented by 1. A history record is created to correspond to each batch. The records are sorted on every run and checked to ensure the batch numbers are in incremental order with no skipped numbers. Within the batch, DOR's Individual Income Tax System checks to ensure the number of detail records matches the batch trailer record.

On May 14, 2001 DOR ceased executing the audit control, which would halt (abend) the program when there was a break in batch numbers. This was done after the control program actually identified an issue. It was discovered that the Internet SCNET program was assigning a batch number even if there was no data to transmit for a particular day. As a result of this, no batch would be forwarded to the Individual Income Tax System. When the Individual Income Tax System finally received a batch, the batch number was out of sync with what was expected. This flaw has been corrected and the control is functioning again.

DOR believes this control addresses the "completeness, accuracy and validity of all processing of Internet-filed returns." This ongoing operation of automated controls operating in Production Services is the responsibility of the Production Services Manager.

---

State of South Carolina  
Department of Revenue  
301 Gervais Street, P.O. Box 125, Columbia, South Carolina, 29214

---

01-4 Physical Access Controls

**Department of Revenue**

DOR plans to locate an exercise area directly next to its network equipment room. All Local Area Network equipment is located inside the Network Equipment Room and is separated from the Exercise Room by partitions and heavy-duty mesh wire walls. The wire walls for the Network Equipment Room have a secured door that is locked with only key access. Keys are only provided to authorized personnel. While key locks can provide adequate physical security, risks related to unauthorized access increase since key can be copied. Unsupervised off-hour access to the area that contains the network servers and the SQL servers creates a risk of damage to these servers.

We recommend that DOR include a combination locking mechanism for all entrances where computer-processing hardware is located. Passwords and keys should be given only to authorized information system employees. Passwords should be changed on a 30-day cycle and immediately after employees with access to such areas are terminated.

**Management Comments**

**DOR: Michael Garon, CIO**

IRM Management agrees that adequate physical security is needed for computer processing hardware, wiring closets, and file servers. The room referred to contains the Exercise Room (walled in by partitions), Network Equipment Room (wire walls) and the Inserter/Copier Equipment.

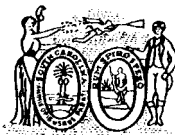
All Local Area Network equipment is located inside the Network Equipment Room and is separated from the Exercise Room by partitions and heavy-duty mesh wire walls. The wire walls for the Network Equipment Room have a secured door that is locked with only key access. Keys are only provided to authorized personnel.

A combination lock mechanism has been considered for the common doorway going into the room where the Exercise Room, Network Equipment Room, and Inserter/Copier Equipment are located. However, at this time DOR management believes the cost of the control out-weighs the material nature of the risk. This will continue to be reviewed to ensure the controls are adequate.



# OFFICE OF STATE TREASURER

GRADY L. PATTERSON, JR.  
STATE TREASURER



P.O. DRAWER 11778  
COLUMBIA, SC 29211  
TEL. (803) 734-2101

118 WADE HAMPTON OFFICE BUILDING  
COLUMBIA, SC 29201

December 11, 2001

Joy Norman  
Deloitte and Touche LLP  
Enterprise Risk Services  
Suite 1500  
191 Peachtree St. NE  
Atlanta, GA 30303-1924

Dear Joy,

In response to the Management Letter comments on the Treasury included in the statewide Data Processing review, we are pleased to provide the following:

The Programmers only have access to the COBOL programs, which comprise only about 20% of our source code. As time permits, we will convert those to Natural. The warrant file is a CG's file and the programmers do not have access to it. Additional controls in place include: all movement of programs is done by the Data Base Administrator, and all requests for changes are signed by a senior manager. Before those changes are put into production, the senior manager must sign-off on the test results. Due to the size of the staff, it is necessary for all programmers to share in the nightly maintenance responsibilities; therefore we feel the current access is necessary.

Sincerely,

A handwritten signature in cursive script that reads "Willie F. Pratt".

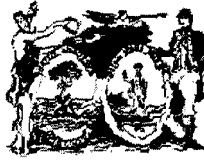
Willie F. Pratt  
Senior Assistant State Treasurer

STATE OF SOUTH CAROLINA  
**State Budget and Control Board**  
OFFICE OF INFORMATION RESOURCES

JIM HODGES, CHAIRMAN  
GOVERNOR

GRADY L. PATTERSON, JR.  
STATE TREASURER

JAMES A. LANDER  
COMPTROLLER GENERAL



HUGH K. LEATHERMAN, SR.  
CHAIRMAN, SENATE FINANCE COMMITTEE

ROBERT W. HARRELL, JR.  
CHAIRMAN, WAYS AND MEANS COMMITTEE

FRANK FUSCO  
EXECUTIVE DIRECTOR

4430 Broad River Road  
COLUMBIA, SOUTH CAROLINA 29210  
(803) 896-0300

MATTHEW R. DEZEE  
CHIEF INFORMATION OFFICER

January 24, 2002

Mr. Wayne Sams  
State Auditor Office  
1401 Main Street, Suite 1200  
Columbia, SC 29201

Dear Mr. Sams:

Mary McKessick of Deloitte and Touche requested that I respond to you as to the Office of Information Resources' response to the Deloitte and Touche audit concerning 01-6 Disaster Recovery/Business Continuity Planning. The following is our response.

We are in full agreement that the recovery of services needs to be tested with the Sunguard disaster recovery hot site. The State Data Center has scheduled this testing with Sunguard for the first quarter of fiscal year 2002. OIR has requested from the state agencies supported by the data center, that they provide the business continuity plans for their applications to be incorporated into the disaster recovery plan. OIR can not complete this part of the disaster recovery plan without input from state agencies.

I hope this clarifies the current status of the "Disaster Recovery Plan". If you need further assistance or information, please feel free to ask.

Warm regards,

A handwritten signature in cursive script that reads "Dave Gerth".

Dave Gerth, Deputy Director, ISO  
Office of Information Resources

DG/paw

Katie Morgan  
Deputy Director / Administration  
(803) 896-0515  
(803) 896-0099 FAX

Tom Fletcher  
Deputy Director / TELCO  
(803) 896-0404  
(803) 896-0097 FAX

Dave Gerth  
Deputy Director / ISO  
(803) 896-0162  
(803) 896-0091 FAX



2600 Bull Street  
Columbia, SC 29201-1708

March 1, 2002

COMMISSIONER:  
C. Earl Hunter

Mr. Tom Wagner, CPA  
State Auditor  
1401 Main Street, Suite 1200  
Columbia, South Carolina 29201

BOARD:  
Bradford W. Wyche  
Chairman

Mark B. Kent  
Vice Chairman

Howard L. Brilliant, MD  
Secretary

Carl L. Brazell

Louisiana W. Wright

L. Michael Blackmon

Larry R. Chewning, Jr., DMD

Dear Mr. Wagner:

We have reviewed the two audit findings for the FY2001 Statewide Single Audit for the S.C. Department of Health and Environmental Control, and offer the following responses for your consideration.

#### **01-7. Security Policies and Procedures**

**Recommendation:** We recommend that DHEC develop formal information security policies and accompanying procedures and communicate the policies to all employees with access to computer systems. In developing the policies, management should:

- Review the types and uses of all system resources and classify them according to importance and sensitivity, and
- Provide user education and communication of the security policies.

DHEC should, at a minimum, document and implement security administration procedures which:

- Assign responsibility for maintaining and enforcing security administrative procedures.
- Define user responsibility for the information used and processed.
- Require written management approval for granting access authorities and ensure timely changes to employee access after terminations or transfers.
- Specify password requirements.
- Provide for periodic review of security violations.

**Action Taken:** We agree that an updated security policy is needed and we will begin development. Over the years, additional computer platforms have been implemented into the Agency's computing network and we have not only the IBM mainframe computer, but also the AIMS / ORACLE environment, the AS-400 environment, all of

the Local Area Networks (LANs) and Windows NT Database Servers. A single corporate policy for these diverse systems will be developed.

Currently, the main entry screen for mainframe access has a Net Manager option that lists all the mainframe applications. The option is available to all users with mainframe access and each application has a documentation page that explains what the application is and details the procedures needed to gain access. The content of these pages changes as the procedures change and we rely upon users' open access to the on-line documentation rather than numerous hard copies required to accomplish the same task.

Each system added to a platform is always subject to security restrictions requested by the originating sponsor and access always requires sign-off by the sponsor, stating the level of security access before any user can gain access. Application owners are responsible for notifying IS security of the degrees of access available to all of their users. Additionally, all employees are required to sign confidentiality statements to emphasize the need for restricted use of information. Password requirements vary between the different operating systems and those are documented in the operating procedures of the different systems.

Because of staff and time constraints, these various procedures have not been pulled together into a single operating procedures manual. Though operating practices, access is tightly restricted and we believe that the level of security is appropriate for the intended use for each of the applications.

The development of agency-wide information security policies and procedures has been incorporated into the agency's HIPAA Compliance project. These policies and procedures will be developed to comply with HIPAA requirements and to meet the HIPAA Privacy Rule timetable of April 14, 2003. These policies will be incorporated into the agency Administrative Policy Manual, which is published on-line and available to all agency staff with computer access. Procedures to support these policies will be developed to meet the specific requirements of our various information systems and published in an Information Systems Security Procedures manual. This manual will also be developed to meet the HIPAA Privacy Rule timetable of April 14, 2003.

#### **01-8. Granting/Removal of Employee Access-AIMS**

**Recommendation:** We recommend that DHEC implement procedures to ensure that systems access for transferred or terminated employees is updated or removed in a timely manner. Consider generating a list of terminated and transferred employees from the Human Resource system on a monthly basis and distributing the list to the data base administration manager for access updating/removal.

**Action Taken:** A monthly listing of terminated employees is already produced and those with AIMS access are removed. Because of the lack of work responsibility information on transfers, it will not be practical to use names from that file. However, IS will

communicate the need for all supervisors of a transferred position to notify central management of the transfer so that adjustments to the person's security access can be changed.

As indicated above, a monthly listing of terminated employees is provided to the AIMS database administrators and access is revoked for those employees. Another list of terminated and transferred employees is provided to the mainframe Security Administrator and access is revoked or changed for these employees.

Agency-wide policies and procedures to address changes to systems access for employee's transfers and terminations will be developed as part of the agency's HIPAA Compliance project, scheduled for April 14, 2003. Policies will address access to all information systems. Procedures will be based on the specific requirements of the various information systems.

In the near term, IS will publish, through the Bureau of Personnel, a communication to all personnel coordinators emphasizing the need to notify both local and central security administrators of transferred or terminated employees, so that the employee's systems access can be terminated or changed.

We appreciate the thorough work of your auditors. If you have any questions, please do not hesitate to contact us.

Sincerely,



C. Earl Hunter  
Commissioner

cc: R. Douglas Calvert, Chief Operating Officer  
John T. Watson, CPA, Director, Bureau of Finance  
Douglas E. Cooper, CGFO, Assistant Director, Bureau of Finance  
Bob Arndt, Director, Bureau of Information Systems  
Mary I. Fuhrman, CPA, CIA, Director, Office of Internal Audits

64 copies of this document were published at an estimated printing cost of \$1.64 each, and a total printing cost of \$104.96. The FY 2001-02 Appropriation Act requires that this information on printing costs be added to the document.